УДК 351.74

Т. С. Вайда
доцент кафедри спеціальної фізичної та вогневої підготовки Херсонського факультету Одеського державного університету внутрішніх справ, кандидат педагогічних наук, доцент (Україна)

МЕТОДИКА РОЗПІЗНАВАННЯ ПРАЦІВНИКАМИ КІБЕРПОЛІЦІЇ УКРАЇНИ ФЕЙКІВ, КОТРІ СТВОРЮЮТЬСЯ ДЕЯКИМИ ЗАСОБАМИ МАСОВОЇ ІНФОРМАЦІЇ

Методика распознавания работниками киберполиции Украины фейков, которые создаются некоторыми средствами массовой информации

В статье рассмотрена актуальная проблема защиты информационной независимости Украины — способы борьбы киберполиции государства с существованием в некоторых средствах массовой информации неправдивых материалов (фейков) относительно освещения событий, которые происходят в современных условиях в связи с оккупацией территории отдельных районов Донецкой и Луганской областей и аннексией АР Крым, проведением антитеррористической операции и т. п.

На основе проведенного анализа профессиональной литературы и публикаций экспертов на страницах Интернет-ресурсов по проблеме исследования рассмотрен комплекс способов, которые применяются отдельными медиасредствами для создания неправдивой информации: 1) использование фотографий, которые не отображают истинное положение дел в конкретной социально-политической ситуации (стране, местности и т. п.) — изображение событий, которые происходили на территории другого государства, демонстрация фотографий людей, которые являются непричастными к рассматриваемой журналистом проблеме; 2) замена авторских высказываний свидетеля, у которого берут интервью, словами корреспондента или комментариями журналиста с другим содержанием, при этом кадры репортажа показываются в телеэфире с демонстрацией фотографии этого человека (или на фоне беседы с ним); 3) подмена начального содержания текста очевидцев или использование свидетельств лиц, которые не причастны к этому событию (постановочные кадры); 4) апеллирование к сообщениям авторитетных западных СМИ, которые информацию такого содержания о конкретном событии не публиковали.

Предложены некоторые рекомендации (способы проверки) относительно опровержения ложной информации (фейков), которая создается отдельными СМИ: 1) поиск использованного медиасредством изображения, которое вызывает подозрение, в браузере Google; 2) переход на оригинальный медиаресурс для получения более достоверной информации об использованном электронным СМИ сомнительном видеоролике; 3) учет даты размещения видеоматериала на Интернет-ресурсе, анализ комментариев под ним, которые сделаны пользователями; конкретизация деталей фото- или видеосюжета (названия объектов, автомобильные номера, таблички с названиями улиц и т. д., по которым часто можно определить истинное положение местности, о которой идет речь в сюжете); 4) использование пользователем (работником киберполиции) ключевых слов для описания показанного в видеоматери-

але события со следующим их введением в поисковике на YouTube или Google (метод опровержения перекрученного социального значения события, которое применяется некоторыми СМИ путем вырывания части сюжета из контекста прилагаемой информации о нем в целом для дальнейшего использования в Интернет-ресурсе с другой целью); 5) выполнение скриншота наиболее показательного (яркого) кадра из видеосюжета и размещение его в поисковике картинок в Google по описанному выше способу; 6) критический анализ свидетельств очевидцев, которые в кадре подтверждают тезисы сделанного журналистом сомнительного репортажа, концентрация внимания на личности этого очевидца, которого можно было встретить раньше в аналогичных проблемно-дискуссионных видеоматериалах; 7) опровержение сообщенной в медиаресурсах информации, которая подается со ссылкой на авторитетные западные СМИ для усиления правдоподобия или подчеркивания значимости определенного события (способ развенчивания фейков, авторы которых ссылаются для подтверждения достоверности информации на малоизвестные маргинальные сайты; выявление искажений в трактовке реальных событий, которые сообщаются СМИ с надежной репутацией).

Сделан вывод, что главными условиями для эффективного распознавания фейков являются: 1) критическое отношение пользователей (работников киберполиции) к размещенной в Интернет-ресурсах информации, которая воспринимается рядовыми гражданами на веру; 2) определение правдивости материала о событии путем сопоставления информации из разных источников (печатных СМИ, теленовостей, медийных ресурсов, показаний очевидцев и т. п.).

Methods of recognition by Ukraine's worker cyberpolice of fakes, which are created by some mass media

The issue of the day of defence of informative independence of Ukraine is considered in the article — fight of the state's cyberpolice against existence in some mass medias of untruthful materials (fakes) in relation to presentation of events which take place in modern terms in connection with occupation of territory of some districts of Donetsk and Luhansk regions and by annexation of AR of Crimea of the Ukrainian state, by realization of anti-terror operation etc.

On the basis of analysis of professional literature and publications of experts on the Internet resources the complex of methods which are used by separate media facilities for creation of untruthful information is considered: 1) use of pictures, which do not represent veritable state of matter in the definite situation (in the country, localities etc.) — image of events which took place on the territory of other state, or demonstration of pictures of people which are not implicated to the problem examined by a journalist; 2) replacement of authorial utterances of a man who is taken an interview, by the words of a correspondent or by the comments of journalist with other maintenance, whose shots with the use of a picture of this man are shown or on a background of the interview with him; 3) substitution of initial maintenance of text of eyewitnesses or use of certificates of persons who do not have involvement to this event (raising shots); 4) appealing to the reports of authoritative western mass-media, which information of such maintenance about a concrete event did not report.

Some recommendations (methods of verification) in relation to refutation of untruthful information (fakes), which are given by some mass-media are offered: 1) search of the image which causes suspicion used by a mean of medias, in the browser of Google; 2) pass-

ing to the original mediaresource for the receipt of more truthful information about used by electronic mass-media doubtful videofragment; 3) account of date of placing of video data on the Internet-resource, analysis of comments which are done by users under it; specification of details of a photo- or videoplot (names of objects, motor-car numbers, plates with the names of streets, on which it is often possible to define veritable position of locality about which is spoken in a plot); 4) the application by the user (by the worker of cyberpolice) of keywords for description of the event represented in video data with their further introduction in a search on YouTube or Google (method of refutation of twisting of social value of event which is used by some mass-media by the method of pulling out of a part of the plot from the context of the reported information about it on the whole for further presentation in an Internet-resource with other purpose); 5) implementation of screenshot of the most model (bright) picture from a videoplot and it's apartment in the search of images in Google by the method described above; 6) walkthrough of certificates of eyewitnesses who confirm the theses of the doubtful reporting done by a journalist, attracting attention on a personality of an eyewitness who could be met before in analogical problem-debatable videomaterials; 7) refutation of the information which is given with the reference to authoritative western mass-media for strengthening of plausibility or underlining of meaningfulness of certain event (method of dethronement of fakes, authors of which refer for validifying of information on marginal sites; an exposure of twisting in interpretation of the real reports which are revealed by mass-media with reliable reputation).

The conclusion is done that main terms for effective recognition of fakes are: 1) critical attitude of users (workers of cyberpolice) toward the information placed in the Internet-resources which is perceived by ordinary citizens on a faith; 2) determination of veracity of material about an event by comparison of information from different sources (printed mass-media, televisional news, internet-resources, certificates of eyewitnesses etc).

В статті розглянуто актуальну проблему захисту інформаційної незалежності України — способи боротьби кіберполіції держави з існуванням у деяких засобах масової інформації (далі − ЗМІ) неправдивих матеріалів (фейків) щодо висвітлення подій, котрі відбуваються у сучасних умовах у зв'язку із окупацією території окремих районів Донецької і Луганської областей та анексією АР Крим, проведенням антитерористичної операції (далі — АТО) тощо.

На основі аналізу фахової літератури та публікацій експертів на сторінках Інтернет-ресурсів розглянуто комплекс способів, котрі застосовуються окремими медійними засобами для створення неправдивої інформації: 1) використання фотографій, які не відображують істинне положення справ у конкретній ситуації (країні, місцевості тощо) — зображують події, які відбувалися раніше чи на території іншої держави, або демонстрація фотографій людей, котрі є непричетними до розглядуваної журналістом проблеми; 2) заміна авторських висловлювань особи, у котрої беруть інтерв'ю, словами кореспондента чи коментарями журналіста іншого змісту, при цьому кадри репортажу з останніми показуються в телеефірі з демонстрацією фотографії цієї особи (на фоні бесіди з нею); 3) підміна початкового змісту тексту очевидців або використання свідчень осіб,

які не мають причетності до цієї події (постановочні кадри); 4) апелювання до повідомлень авторитетних західних ЗМІ, котрі не оприлюднювали інформацію такого змісту про конкретну подію.

Запропоновано деякі рекомендації (способи перевірки) щодо спростування неправдивої інформації (фейків), котрі подаються окремими ЗМІ: 1) пошук використаного медійним засобом зображення, що викликає підозру, у браузері Google; 2) перехід на оригінальний медіаресурс для отримання більше достовірної інформації про застосований електронним ЗМІ сумнівний відеоролик; 3) врахування дати розміщення відеоматеріалу на Інтернет-ресурсі, аналіз змісту коментарів під ним, котрі зроблені користувачами; конкретизація деталей фото- чи відеосюжету (назви об'єктів, автомобільні номери, таблички з назвами вулиць тощо), за якими часто можна визначити істинне розміщення місцевості, про котру йде мова у сюжеті); 4) використання користувачем (працівником кіберполіції) ключових слів для опису події, зображеної у відеоматеріалі, з наступним їх введенням у пошук YouTube або Google (метод спростування перекручування соціального значення події, котре застосовується окремими ЗМІ завдяки використанню частини сюжету, котра вирвана з загального контексту повідомленої інформації про подію в цілому, для подальшого подання в Інтернет-ресурсі з іншою метою); 5) виконання скріншоту найбільш показового (яскравого) кадру із відеосюжету та розміщення його в пошук зображень в Google за описаним вище способом; 6) критичний аналіз свідчень очевидців, котрі підтверджують тези зробленого журналістом сумнівного репортажу, концентрація уваги на особистості очевидця, який зустрічався раніше в аналогічних проблемно-дискусійних відеоматеріалах; 7) спростування повідомленої у медійних ресурсах інформації, котра подається із посиланням на авторитетні західні ЗМІ для підсилення правдоподібності або підкреслення значимості певної події (спосіб розвінчування фейків, автори котрих посилаються для підтвердження достовірності інформації на маргінальні сайти; виявлення перекручувань у трактуванні реальних повідомлень, котрі оприлюднюються ЗМІ з надійною репутацією).

Зроблено висновок, що головними умовами для ефективного розпізнавання фейків є: 1) критичне ставлення користувачів (працівників кіберполіції) до розміщеної в Інтернет-ресурсах інформації, котра сприймається пересічними громадянами на віру; 2) визначення правдивості матеріалу про подію шляхом зіставлення інформації з різних джерел (друкованих ЗМІ, теленовин, медійних ресурсів, свідчень очевидців тощо).

Актуальність проблеми. Республіку Україну її Конституція (стаття 5 Основного Закону) визначає як суверенну і незалежну, демократичну, соціальну та правову державу [1], яка в своєму становленні пройшла складні випробуван-

ня і в сучасних умовах протистоїть серйозним внутрішнім та зовнішнім викликам на Півдні й Сході своїх границь щодо захисту державного суверенітету, територіальної цілісності та недоторканності державних кордонів, вирішує складні соціально-політичні проблеми подальшого розвитку державності й громадянського суспільства. При цьому людина, її безпека визнаються в Україні найвищою соціальною цінністю, а захист та гарантування національної безпеки для всього населення країни визначають зміст і спрямованість діяльності правоохоронних органів держави, складають її головний обов'язок та визначають високий рівень відповідальності перед громадянином.

Виходячи з положень Доктрини інформаційної безпеки України, ми погоджуємося із точкою зору її авторів, що застосування Російською Федерацією технологій гібридної війни проти української держави перетворило інформаційну сферу на ключову арену протиборства. Саме проти України використовується найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [2].

Значна частина інформації із характеристикою соціально-політичних процесів, які відбуваються в Україні, зокрема, стосовно висвітлення резонансних подій (наприклад, бойових дій при проведенні АТО на Сході української держави, під час анексії Криму тощо) не відповідають дійсності. За результатами моніторингу громадської організації «Інститут масової інформації» (далі — ІМІ) у січні 2017 року, 10 % новин на інформаційних сайтах терористичних організацій окремих районів Донецької і Луганської областей (далі — ОРДЛО) є відвертою брехнею. При цьому 82 % матеріалів про окупаційну владу в інтернет-ЗМІ на непідконтрольних українській владі територіях Донбасу є компліментарними, 18 % — нейтральні, проте критичних матеріалів немає взагалі [3].

Згідно з результатами досліджень організації ІМІ, загалом близько 20 % новин на місцевих сайтах присвячені окупаційній владі, тоді як про українську владу матеріалів більше — 32 % повідомлень. І переважна кількість цих матеріалів (87 %) негативно забарвлені, 13 % — нейтральні, а позитивних матеріалів не було виявлено взагалі. У той же час, за даними аналітиків, діяльності російської влади присвячено в середньому 8 % новин, причому у переважній кількості вона теж висвітлюється позитивно (91 % новин), негативні або критичні матеріали — відсутні [3].

Головною причиною цього негативного соціального явища є застосування окремими ЗМІ матеріалу з метою ведення пропагандистської діяльності проти державності України: в такому випадку повідомлення новин використову-

ються не для інформування громадян, а для нав'язування їм точки зору, котра вигідною проросійським силам.

В контексті піднятої нами проблеми та у відповідності до вимог статті 7 Закону України «Про основи національної безпеки України» до загроз національним інтересам і національній безпеці України в інформаційній сфері відносять: прояви обмеження свободи слова та доступу громадян до інформації; поширення ЗМІ культу насильства, жорстокості; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [4].

На практиці в сучасних умовах простежуються спроби окремих ЗМІ (в першу чергу іноземних, на окупованих ОРДЛО, в АР Крим) викривляти державну політику щодо територіальної цілісності та незалежності України, пропагувати ідеї сепаратизму; збільшується кількість фейків.

Проведений аналіз ряду наукових робіт вітчизняних вчених дає підстави констатувати, що потенційні можливості ЗМІ в частині їх впливу на формування суспільства чи певних її суб'єктів були предметом вивчення та монографічних досліджень багатьох науковців. За результатами їх узагальнення можна виділити наступні напрямки діяльності сучасних медіаресурсів та їх значення у соціальному житті країни: 1) роль засобів масової комунікації у виборчому процесі як інструмент моделювання політичної свідомості розглядували О. О. Заславська, О. А. Семченко та ін.; 2) дослідження моделі медіаполітичної системи у сучасній Україні, інформаційного розвитку та глобалізації комунікаційного простору здійснювали С. В. Демченко, Т. Я. Лильо та ін.; 3) можливості впливу мас-медіа на створення та функціонування стереотипів масової свідомості аналізували М. В. Бутиріна, І. А. Чудовська-Кандиба та ін.; 4) освітньо-виховну роль ЗМІ як чинника формування людини обґрунтовували А. М. Бахметьєва, І. І. Курліщук, С. І. Семчук та ін.; 5) проблемою свободи преси та її впливу на формування соціуму переймалися В. М. Гвоздєв, О. В. Кабачна, Б. І. Мотузенко, Н. Хомский та ін.; 6) методи діяльності та форми взаємодії ЗМІ з суб'єктами державного управління вивчали Н. В. Коритнікова, Я. О. Легеза, О. І. Трухачов та ін.; 7) роль та значення засобів масової комунікації у системі соціалізації окремих верств населення (вихованні суспільно орієнтованого способу життя) аналізували А. А. Согорін, Н. С. Удріс та ін.

В свою чергу окремі суб'єкти вітчизняного медіапростору недостатньо уваги приділяють спростуванню цієї неправдивої інформації, не протистоять їй висвітленням проявів масових випадків патріотизму та героїзму українського народу при проведенні АТО на сході України; недостатньо використовується стратегічний наратив — спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію тощо [2].

Метою роботи є: 1) виявлення та проведення критичного аналізу використовуваних інтернет-ЗМІ методів деструктивного впливу, які зорієнтовані на хибне інформування населення України; 2) надання рекомендацій правоохоронним органам (кіберполіції) для удосконалення нагляду за діяльністю вітчизняних та зарубіжних медіазасобів з метою попередження існуючих загроз для національної безпеки України в інформаційній сфері; 3) визначення способів розпізнавання неправдивої інформації, яка подається в окремих медійних засобах.

Результати дослідження. У відповідності з положеннями Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № 47/2017, комплексний характер актуальних загроз національній безпеці України в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [2]. Одним із способів негативного впливу на формування свідомості громадян української держави є створення та поширення деякими ЗМІ неправдивої інформації (фейків) про суспільно-політичні події в Україні чи неадекватне їх трактування.

Перш за все розглянемо основні методи розпізнавання неправдивої інформації — фейків (від англ. слова «fake» — підробка, фальсифікація, обман, тобто неправдиві новини, котрі не всі пересічні громадяни можуть відрізнити від правди), які подаються в окремих ЗМІ.

Для отримання істинного уявлення про суспільні чи міжнародні події читачам (або блокування інформації працівниками кіберполіції) необхідно, на нашу думку, працювати з доведеними (достовірними) фактами, а не з твердженнями суб'єктивної точки зору окремого суб'єкта ЗМІ, який їх опублікував. Наприклад, якщо антиукраїнська сторона заявляє про деяку надзвичайну подію в Україні, а вітчизняні Міністерство зовнішніх справ або Міноборони української держави цю інформацію спростовують без надання доказів своєї позиції, то читач потрапляє в ситуацію «слово проти слова» — дві зацікавлені сторони говорять про вигідне для кожної з них своє трактування проблеми. Тому стосовно діяльності авторитетних медійних ресурсів спостерігається мало словес-

них спростувань, репортажі містять обґрунтовану інформацію, котра підкріплена фото- чи відеофактами.

Розглянемо способи виявлення неправдивої інформації, котрими можуть скористатися як працівники кіберполіції у боротьбі з її поширенням, так і пересічні громадяни для адекватного аналізу й усвідомлення суспільних процесів.

1. Спростування фотофейку. Фотофейк є найбільш розповсюдженим і в той же час — найбільш легким для спростування типом неправдивої інформації. Як правило, визначити істинність окремої фотографії в Інтернеті можна протягом декількох секунд. Але, як виявляється на практиці, значна кількість громадян та навіть працівників кіберполіції (користувачів Інтернету) не знають чи не вміють це робити і довіряють кожній «резонансній» фотографії [5].

Для розпізнання фотофейку є *декілька способів*.

У випадку користування браузером Google Chrome, користувачеві достатньо клікнути по фотографії, яка викликає у нього підозру, правою кнопкою миші і вибрати пункт «Знайти це зображення в Google».

При користуванні іншим браузером, у котрому по замовчуванню немає функції пошуку за зображенням, можна встановити для цього спеціальний плагін, котрих досить багато. Наприклад, добре працює плагін «Who stole my pictures» (у вітчизняному варіанті «Хто вкрав мої картинки»). Корисною властивістю цього плагіна є те, що він вміє шукати не тільки по браузеру Google, але й по Яндексу, Tineye або по всім трьом одночасно.

Якщо відсутній Chrome і немає можливості встановити плагін, можна провести перевірку таким способом: у будь-якому браузері потрібно поряд з вкладкою з відкритим сайтом з підозрілою фотографією, відкрити ще одну, в котрій активізувати розділ з картинками Google. Після цього потрібно вернутися у попередню вкладку, «схопити» комп'ютерною мишкою потрібне зображення, перетягнути його у вкладку Google та відпустити у строчці пошуку.

У результаті застосування цього методу користувач (працівник кіберполіції) перевіряє одразу два дуже важливих аспекти: 1) чи є картинка оригінальною або ж піддавалась обробці у фоторедакторі (наприклад, було дорисовано якийсь елемент з метою використання її як ілюстрації до потрібного сюжету); 2) інший важливий момент, котрий можна перевірити таким способом — дата публікації фотографії, а також те, що на ній насправді зображено (наприклад, заміна наслідків бойових дій в Сирії на українські).

2. Спростування відеофейку. Працювати працівникам Національної поліції (підрозділів кіберполіції) з таким фейком складніше, ніж з фотографіями, оскільки простого способу пошуку за критерієм «відео» немає. Якщо користувач (працівник кіберполіції) запідозрив, що знайдений відеоматеріал є неправдивим, варто користуватися наступними методами:

1) у випадку виявлення на якомусь сайті вбудованого вікна YouTube варто перейти безпосередньо на цей Інтернет-ресурс, щоб отримати про відеоролик більше інформації (для цього треба клікнути на логотип відеосервісу у правому нижньому куті);

2) настільки простих помилок в діяльності ЗМІ дуже мало. Якщо очевидних ознак відеофейку немає, доцільно звернути увагу на наступне: при зазначенні у назві відео недавньої дати і до того ж цей ролик багатократно розміщується на YouTube протягом короткого періоду часу — є висока ймовірність щодо визначення його фейком.

Обравши відеоролик з найбільшою кількістю переглядів, корисно почитати до нього коментарі — такий прийом є способом виявлення Інтернет-користувачами оригіналу відеосюжету, зокрема, завдяки розміщенню зроблених посилань на нього або участі в обговоренні.

Крім того, доцільно звертати увагу при перегляді відеоматеріалу на окремі деталі — назви об'єктів, автомобільні номери, вуличні таблички. За ними часто можна визначити місцевість, котру насправді зображено (наприклад, проведене розслідування дасть змогу уточнити істинне положення справи, географію місця події тощо);

3) наступний спосіб виявлення фейку: користувач може описати ключовими словами зображене на відео і ввести їх в пошук на YouTube або Google. Таким чином, перекручування значення події чи вирване з контексту її трактування може бути використане ЗМІ з іншою (протилежною) метою;

4) четвертий спосіб: можна зробити скриншот найбільш показового (яскравого) кадру із відеосюжету і завантажити його в пошук зображень у Google за описаним вище прийомом. Є ймовірність того, що коли журналіст готував новину з цим відеоматеріалом та використовував яскравий скриншот в якості ілюстрації, за цим зображенням можна знайти безпосередньо й саме першоджерело.

3. Критична оцінка свідчень очевидців. Часто свідчення безпосередніх свідків події перевірити важко або неможливо, але бувають й винятки. Необхідно вслухатися у зміст мовлення таких осіб — чи є в їх мові підтвердження тез, котрі намагаються донести журналісти (автори новини), або вони говорять про загальні речі, котрі ЗМІ потім використовують у своїх вузьких цілях. Також варто звертати увагу на особу очевидця — чи не бачили його раніше в аналогічних скандальних чи провокаційних репортажах.

4. Перевірка посилань на авторитетні західні ЗМІ. Цей прийом часто використовується окремими медіазасобами для підсилення правдоподібності або авторитетності певного повідомлення. Тим не менш, серед інформаційних по-

відомлень на практиці зустрічається значна кількість гіпотетичних припущень від різноманітних маргінальних сайтів, авторитетність котрих варто перевіряти.

Інший варіант — перекручування реальних повідомлень авторитетних ЗМІ, виривання окремих фраз з загального контексту та маніпулювання ними. Тому завжди потрібно намагатися знайти оригінал новин [6].

Головною умовою для розпізнавання фейку, є, на нашу думку, критичне ставлення до інформації, котра сприймається працівниками кіберполіції чи читачами (користувачами Інтернет-ресурсів). Інформаційна війна є вкрай важливим елементом протистояння між країнами, тому необхідно прагнути не сприймати на віру будь-які повідомлення, а впевнюватися у їх достовірній правдивості [7; 8].

Отже, провівши аналіз можливих способів повідомлення неправдивої інформації (фото- та відеофейків), яка подається деякими деструктивними ЗМІ, нами виділено серед них такі найбільш типові: 1) використання фотографій, які не відображують істинне положення справ у конкретній соціально-політичній ситуації (країні, місцевості тощо) чи наводять подібні до неї зображення іншої території або людей; 2) фотозображення чи показ інтерв'ю з особою, в котрому (інтерв'ю — уточнено нами) відбувається заміна авторських висловлювань словами кореспондента чи коментарями журналіста (за кадром) з іншим змістом; 3) повна підміна свідчень очевидців або використання змісту повідомлення осіб, які не мають причетності до цієї події (т. зв. постановочні кадри); 4) апелювання до повідомлень західних ЗМІ, але котрі таку інформацію про дану подію не оприлюднювали.

Серед основних рекомендацій щодо застосування окремих методів перевірки та спростування неправдивої інформації (фейків) можна виділити наступні: 1) спосіб пошуку конкретного зображення в браузері Google для розвінчування фотофейку, котрий викликає сумніви чи підозру; 2) здійснення переходу на оригінальний браузер з метою визначення відеофейку та отримання про цей відеоролик більше достовірної інформації; 3) звернення уваги на дату розміщення відеоматеріалу на Інтернет-ресурсі та аналіз коментарів, котрі зроблені під ним користувачами; вивчення окремих деталей відеоматеріалу (назв об'єктів, автомобільних номерів, табличок з назвами вулиць, за якими часто можна встановити прив'язку події до певної місцевості); 4) використання користувачем (працівником кіберполіції) опису за ключовими словами зображеного на відео, введення їх в пошук YouTube або Google (спосіб спростування викривлення змісту інформації або неадекватного трактування вирваного з контексту її значення, котрий може бути застосованим окремими ЗМІ з деструктивною метою); 5) виконання скриншот найбільш показового (яскравого) кадру із сумнівного відеоматеріалу з наступним розміщенням його в пошук зобра-

жень в Google з метою перевірки його на достовірність описаним вище способом; 6) аналіз свідчень очевидців, котрі підтверджують чи спростовують тези журналістів, а також звернення уваги безпосередньо на особистість самого очевидця, котрого можна було побачити раніше в подібних провокативних репортажах; 7) пошук та дослідження оригінальних (початкових, вихідних — *уточнено нами*) медіаресурсів, на котрі здійснюють посилання деякі ЗМІ для підсилення правдоподібності або авторитетності своїх повідомлень. Результатом застосування такого методу може бути виявлення недостовірної інформації, котра подається маргінальними сайтами; інший варіант подання неправдивої інформації — перекручування сумнівними медіаресурсами реальних повідомлень, котрі подаються авторитетними ЗМІ.

Головними умовами для ефективного розпізнавання фейків, на нашу думку, є такі: 1) критичне ставлення користувачів та працівників кіберполіції до розміщеної в Інтернет-ресурсах інформації, котра сприймається широким загалом на віру; 2) визначення правдивості матеріалу про події шляхом зіставлення інформації з різних джерел (друкованих ЗМІ, теленовин, медійних ресурсів, показів очевидців тощо).

У протистоянні між ворогуючими країнами не варто недооцінювати роль та значення сучасних методів ведення інформаційної війни, в котрі держава-агресор втягує й окремі ЗМІ. Вміння громадян України та працівників кіберполіції своєчасно виявляти провокаційні (фейкові) повідомлення дають змогу правильно сприймати реальні події, проявляти адекватне (критичне) ставлення до них, формувати на цій основі відповідну суспільну думку українського народу та відображувати її в державницькій й громадсько-патріотичній позиції.

Список основних джерел

1. Конституція України : прийнята на п’ятій сесії Верховної Ради України від 28 червня 1996 року (із змінами, внесеними Законом України від 21 лютого 2014 року № 742-VII) [Електронний ресурс]. — Режим доступу: http://zakon0.rada.gov.ua/laws/show/254к/96-вр. — Дата доступу: 03.03.2017. Вернуться к статье

2. Доктрина інформаційної безпеки України : Указ Президента України, 25 лютого 2017 р. № 47/2017 [Електронний ресурс]. — Режим доступу: http://www.president.gov.ua/documents/472017-21374. — Дата доступу: 03.03.2017. Вернуться к статье

3. IMI: Кожна 10-та новина на сайтах ОРДЛО — фейк [Електронний ресурс]. — Режим доступу: http://www.pravda.com.ua/news/2017/02/24/7136338/. — Дата доступу: 03.03.2017. Вернуться к статье

4. Про основи національної безпеки України : Закон України, 19 червня 2003 р., № 964-IV : із змін. та доп. станом на 16.07.2015 г. // Голос України. — 2003. — № 134. — С. 20–21. Вернуться к статье

5. Фейк. Основные методы распознания неправды в СМИ [Електронний ресурс]. — Режим доступу: http://antikor.com.ua/articles/6885-fejk._osnovnye_metody_raspoznanija_nepravdy_v_smi. — Дата доступу: 03.03.2017. Вернуться к статье

6. Борьба с неправдивой информацией о событиях в Украине [Електронний ресурс]. — Режим доступу: http://www.stopfake.org. — Дата доступу: 03.03.2017. Вернуться к статье

7. Вайда, Т. С. Засоби масової інформації як чинник формування правової свідомості правоохоронців / Т. С. Вайда // Правова держава: історія, сучасність та перспективи формування в Україні : матеріали III-ї Всеукраїнської наук.-практ. конф., 23 квітня 2010 р., Запоріжжя : у 2-х ч. — Запоріжжя : Юридичний інститут ДДУВС, 2010. — Ч. II. — С. 193–196. Вернуться к статье

8. Вайда, Т. С. Організаційно-профілактична діяльність правоохоронних органів щодо попередження деструктивних впливів засобів масової інформації на формування суспільної думки в сучасних умовах / Т. С. Вайда // Держава і право незалежної України: здобутки та перспективи : матеріали Всеукр. наук. конф., Одеса, 24 черв. 2016 р. — Одеса : ОДУВС, 2016. — С. 59–61. Вернуться к статье